CLAIMS

1. A method of defining a transformation between an input signal and an output signal, the method comprising the steps of:

(A) allocating said input signal among a plurality of block input signals;

(B) establishing a plurality of transfer functions each configured to present a plurality of unique symbols as a block output signal responsive to said block input signal; and

(C) concatenating said block output signals to form said output signal.

2. The method according to claim 1, wherein step (C) is concatenating said block output signals to form an intermediate result, the method further comprising the step of establishing a second transfer function configured to permutate said intermediate result to present said output signal.

3. The method according to claim 1, wherein said transfer function is a table configured as k columns and 2^k rows

where k is a bit width of said block input signal and each said row stores one of said symbols.

4. The method according to claim 3, further comprising the step of extracting said plurality of symbols stored in said tables from a random source configured such that each said symbol has an approximately equal probability of appearance.

5. The method according to claim 4, further comprising the steps of:

(i) selecting a staring point within said random source to extract said symbols for a first table of said tables;

(ii) calculating a number of symbols extracted for said first said table;

(iii) calculating a subsequent starting point to extract said symbols for a subsequent table of said tables based upon said starting point and said number in response to steps (i) and (ii);

(iv) updating said subsequent starting point based upon said subsequent starting point and said number; and

(v) repeating step (iv) for all remaining said tables.

6. The method according to claim 5, further comprising the step of presenting said bit width and said starting point as a cryptographic key.

7. The method according to claim 1, wherein step (A) is allocating a predetermined number of units of said input signal to each said block input signal.

8. The method according to claim 7, further comprising the step of allocating fewer than said predetermined number of units to one of said block input signals.

9. The method according to claim 1, further comprising the step of establishing a counter configured to produce said input signal.

10. The method according to claim 9, further comprising the steps of:

duplicating said counter and said plurality of transfer functions to produce a plurality of output signals; and

concatenating said plurality of output signals to present a second output signal.

11. An information recording medium for use in a computer to define a transformation between an input signal and an output signal, the information recording medium recording a computer program that is readable and executable by the computer, the computer program comprising the steps of:

(A) allocating said input signal among a plurality of block input signals;

(B) establishing a plurality of transfer functions each configured to present a plurality of unique symbols as a block output signal responsive to said block input signal; and

(C) concatenating said block output signals to form said output signal.

12. The computer program according to claim 11, wherein step (C) is concatenating said block output signals to form an intermediate result, the computer program further comprising the step of establishing a second transfer function configured to permutate said intermediate result to present said output signal.

13. The computer program according to claim 11, wherein said transfer function is a table configured as k columns and 2^k rows where k is a bit width of said block input signal and each said row stores one of said symbols.

14. The computer program according to claim 13, further comprising the step of extracting said plurality of symbols stored in said tables from a random source configured such that each said symbol has an approximately equal probability of appearance.

15. The computer program according to claim 14, further comprising the steps of:

(i) selecting a staring point within said random source to extract said symbols for a first table of said tables;

(ii) calculating a number of symbols extracted for said first said table;

(iii) calculating a subsequent starting point to extract said symbols for a subsequent table of said tables based upon said starting point and said number in response to steps (i) and (ii);

(iv) updating said subsequent starting point based upon said subsequent starting point and said number; and

(v) repeating step (iv) for all remaining said tables.

16. The computer program according to claim 15, further comprising the step of presenting said bit width and said starting point as a cryptographic key.

17. The computer program according to claim 11, wherein step (A) is allocating a predetermined number of units of said input signal to each said block input signal.

18. The computer program according to claim 17, further comprising the step of allocating fewer than said predetermined number of units to one of said block input signals.

19. The computer program according to claim 11, further comprising the step of establishing a counter configured to produce said input signal.

20. A circuit comprising:

means for allocating an input signal among a plurality of block input signals;

means for establishing a plurality of transfer functions each configured to present a plurality of unique symbols as a block output signal responsive to said block input signal; and

means for concatenating said block output signals to form an output signal.